PORTAL
USPTO

THE ACM DIGITAL LIBRARY

◆ Feedback Report a problem Satisfaction survey

Terms used: **password random number encode encrypt encipher**

Found **305 of 216,412**

Sort results by: [relevance ▼]

Display results: [expanded form ▼]

◆ Save results to a Binder
[?] Search Tips
☐ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200
Best 200 shown

Result page: **1** 2 3 4 5 6 7 8 9 10   next

Relevance scale ☐ ◱ ◰ ◼ ◼

1 Cryptography and data security
Dorothy Elizabeth Robling Denning
January 1982 Book
Publisher: Addison-Wesley Longman Publishing Co., Inc.

Full text available: 🗎 pdf(19.47 MB)

Additional Information: full citation, abstract, references, cited by, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

2 Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm
Mihir Bellare, Tadayoshi Kohno, Chanathip Namprempre
May 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 2
Publisher: ACM Press

Full text available: 🗎 pdf(404.99 KB)

Additional Information: full citation, abstract, references, index terms, review

The *secure shell* (SSH) protocol is one of the most popular cryptographic protocols on the Internet. Unfortunately, the current SSH authenticated encryption mechanism is insecure. In this paper, we propose several fixes to the SSH protocol and, using techniques from modern cryptography, we prove that our modified versions of SSH meet strong new chosen-ciphertext privacy and integrity requirements. Furthermore, our proposed fixes will require relatively little modification to the SSH protoc ...

Keywords: Authenticated encryption, secure shell, security proofs, stateful decryption

3
Symmetric and Asymmetric Encryption

Gustavus J. Simmons
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
Publisher: ACM Press
Full text available: .pdf(2.23 MB)   Additional Information: <u>full citation</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

4 Encryption and Secure Computer Networks

Gerald J. Popek, Charles S. Kline
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
Publisher: ACM Press
Full text available: .pdf(2.50 MB)   Additional Information: <u>full citation</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

5 Cryptographic sealing for information secrecy and authentication

David K. Gifford
April 1982 **Communications of the ACM**, Volume 25 Issue 4
Publisher: ACM Press

Full text available: .pdf(1.29 MB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

A new protection mechanism is described that provides general primitives for protection and authentication. The mechanism is based on the idea of sealing an object with a key. Sealed objects are self-authenticating, and in the absence of an appropriate set of keys, only provide information about the size of their contents. New keys can be freely created at any time, and keys can also be derived from existing keys with operators that include Key-And and Key-Or
Keywords: conentional crypto-systems, cryptographic sealing, key, seal, secrecy, unseal

6 Information security issues in an APL application

Bill Hillman
June 1984 **ACM SIGAPL APL Quote Quad , Proceedings of the international conference on APL APL '84**, Volume 14 Issue 4
Publisher: ACM Press
Full text available: .pdf(549.98 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

This paper will describe various methods to secure an APL database application. Primary foci will be in the areas of "physical" protection, and in cryptographic techniques. To that end, distinctions will be made between "data," and "information." Because of those differences, specific methods will be offered which are appropriate for each modality of security. A brief set of examples will be included for the use of IBM's1 RACF

7 Computer security (SEC): Protected transmission of biometric user authentication data for oncard-matching

Ulrich Waldmann, Dirk Scheuermann, Claudia Eckert
March 2004 **Proceedings of the 2004 ACM symposium on Applied computing SAC '04**
Publisher: ACM Press
Full text available: .pdf(574.45 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>

Since fingerprint data are no secrets but of public nature, the verification data transmitted to a smartcard for oncard-matching need protection by appropriate means in order to assure data origin in the biometric sensor and to prevent bypassing the sensor. For this purpose, the verification data to be transferred to the user smartcard is protected with a cryptographic checksum that is calculated within a separate security module controlled by a tamper resistant card terminal with integrated bio ...

Keywords: authentication, biometrics, cryptographic protocols, data integrity, electronic signature, oncard-matching, smartcards, system security, tamper proof environment

8 Intrusion detection: Randomized instruction set emulation to disrupt binary code injection attacks

Elena Gabriela Barrantes, David H. Ackley, Trek S. Palmer, Darko Stefanovic, Dino Dai Zovi
October 2003 **Proceedings of the 10th ACM conference on Computer and communications security CCS '03**
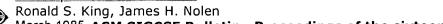**Publisher**: ACM Press

Full text available: pdf(160.71 KB)   Additional Information: full citation, abstract, references, citings, index terms

Binary code injection into an executing program is a common form of attack. Most current defenses against this form of attack use a 'guard all doors' strategy, trying to block the avenues by which execution can be diverted. We describe a complementary method of protection, which disrupts foreign code execution regardless of how the code is injected. A unique and private machine instruction set for each executing program would make it difficult for an outsider to design binary attack code against ...

Keywords: automated diversity, emulation, information hiding, language randomization, obfuscation, security
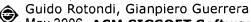
9 A computer ethics course

Ronald S. King, James H. Nolen
March 1985 **ACM SIGCSE Bulletin , Proceedings of the sixteenth SIGCSE technical symposium on Computer science education SIGCSE '85**, Volume 17 Issue 1
Publisher: ACM Press

Full text available: pdf(559.40 KB)   Additional Information: full citation, references, citings, index terms

10 Article abstracts with full text online: A consistent history authentication protocol

Guido Rotondi, Gianpiero Guerrera
May 2006 **ACM SIGSOFT Software Engineering Notes**, Volume 31 Issue 3
Publisher: ACM Press

Full text available: pdf(287.59 KB)   Additional Information: full citation, abstract, references, index terms

Traditional strong authentication systems rely on a certification chain to delegate the authority of trusting an intermediate end. However, in some practical life scenarios a relayed authentication is not accepted and thus it would be advisable a straight proof of trustiness with a direct interaction with the involved party. Our protocol introduces a registry of certified operations from which it descends the authentication and the consequent proof of identity. Despite the fact that such system ...

Keywords: SSL, authentication, dentification, non repudiation, trust

11 Secure password-based cipher suite for TLS

May 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 2
Publisher: ACM Press

Full text available: pdf(507.57 KB)   Additional Information: full citation, abstract, references, citings, index terms, review

SSL is the de facto standard today for securing end-to-end transport on the Internet.

While the protocol itself seems rather secure, there are a number of risks that lurk in its use, for example, in web banking. However, the adoption of password-based key-exchange protocols can overcome some of these problems. We propose the integration of such a protocol (DH-EKE) in the TLS protocol, the standardization of SSL by IETF. The resulting protocol provides secure mutual authentication and key establi ...

Keywords: Authenticated key exchange, dictionary attack, key agreement, password, perfect forward secrecy, secure channel, transport layer security, weak secret

12 Reducing risks from poorly chosen keys

T. Lomas, L. Gong, J. Saltzer, R. Needhamn

November 1989 **ACM SIGOPS Operating Systems Review , Proceedings of the twelfth ACM symposium on Operating systems principles SOSP '89**, Volume 23 Issue 5

Publisher: ACM Press

Full text available: pdf(598.93 KB)   Additional Information: full citation, abstract, references, citings, index terms

It is well-known that, left to themselves, people will choose passwords that can be rather readily guessed. If this is done, they are usually vulnerable to an attack based on copying the content of messages forming part of an authentication protocol and experimenting, e.g. with a dictionary, offline. The most usual counter to this threat is to require people to use passwords which are obscure, or even to insist on the system choosing their passwords for them. In this paper we show alternati ...

13 Password security: a case history

Robert Morris, Ken Thompson

November 1979 **Communications of the ACM**, Volume 22 Issue 11

Publisher: ACM Press

Full text available: pdf(446.89 KB)   Additional Information: full citation, abstract, references, citings

This paper describes the history of the design of the password security scheme on a remotely accessed time-sharing system. The present design was the result of countering observed attempts to penetrate the system. The result is a compromise between extreme security and ease of use.

Keywords: computer security, operating systems, passwords

14 An Efficient One-Way Enciphering Algorithm

H. D. Knoble, C. Forney, F. S. Bader

March 1979 **ACM Transactions on Mathematical Software (TOMS)**, Volume 5 Issue 1

Publisher: ACM Press

Full text available: pdf(803.67 KB)   Additional Information: full citation, references, citings, index terms

15 Computer security: Passwords decay, words endure: secure and re-usable multiple password mnemonics

Umut Topkara, Mikhail J. Atallah, Mercan Topkara

March 2007 **Proceedings of the 2007 ACM symposium on Applied computing SAC '07**

Publisher: ACM Press

Full text available: pdf(287.65 KB)   Additional Information: full citation, abstract, references, index terms

Research on password authentication systems has repeatedly shown that people choose weak passwords because of the difficulty of remembering random passwords. Moreover,

users with multiple passwords for unrelated activities tend to choose almost similar passwords for all of them. Many password schemes have been proposed to alleviate this problem, but they either require modification to the password entry and processing infrastructure (e.g., graphical passwords) or they require the user to have ...

Keywords: authentication, mnemonic sentence, natural language processing, passwords, usability

16 Limitations of the Kerberos authentication system

S. M. Bellovin, M. Merritt
October 1990 **ACM SIGCOMM Computer Communication Review**, Volume 20 Issue 5
Publisher: ACM Press
Full text available: pdf(1.12 MB)   Additional Information: full citation, abstract, citings, index terms

The Kerberos authentication system, a part of MIT's Project Athena, has been adopted by other organizations. Despite Kerberos's many strengths, it has a number of limitations and some weaknesses. Some are due to specifics of the MIT environment; others represent deficiencies in the protocol design. We discuss a number of such problems, and present solutions to some of them. We also demonstrate how special-purpose cryptographic hardware may be needed in some cases.

17 The internet worm program: an analysis

Eugene H. Spafford
January 1989 **ACM SIGCOMM Computer Communication Review**, Volume 19 Issue 1
Publisher: ACM Press
Full text available: pdf(2.45 MB)   Additional Information: full citation, abstract, citings, index terms

On the evening of 2 November 1988, someone infected the Internet with a *worm* program. That program exploited flaws in utility programs in systems based on BSD-derived versions of UNIX. The flaws allowed the program to break into those machines and copy itself, thus *infecting* those systems. This program eventually spread to thousands of machines, and disrupted normal activities and Internet connectivity for many days.This report gives a detailed description of the components of the ...

18 Integrating security in a large distributed system

M. Satyanarayanan
August 1989 **ACM Transactions on Computer Systems (TOCS)**, Volume 7 Issue 3
Publisher: ACM Press

Full text available: pdf(2.90 MB)   Additional Information: full citation, abstract, references, citings, index terms, review

Andrew is a distributed computing environment that is a synthesis of the personal computing and timesharing paradigms. When mature, it is expected to encompass over 5,000 workstations spanning the Carnegie Mellon University campus. This paper examines the security issues that arise in such an environment and describes the mechanisms that have been developed to address them. These mechanisms include the logical and physical separation of servers and clients, support for secure communication ...

19 Cryptography: Password authenticated key exchange using hidden smooth subgroups

Craig Gentry, Philip Mackenzie, Zulfikar Ramzan
November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**
Publisher: ACM Press

Additional Information: full citation, abstract, references, citings, index

Full text available: pdf(300.13 KB)   terms

Existing techniques for designing efficient password authenticated key exchange (PAKE) protocols all can be viewed as variations of a small number of fundamental paradigms, and all are based on either the Diffie-Hellman or RSA assumptions. In this paper we propose a new technique for the design of PAKE protocols that does not fall into any of those paradigms, and which is based on a different assumption. In our technique, the server uses the password to construct a multiplicative group with a (h ...

Keywords: authentication, cryptography, key exchange, password

20 Usability and authentication: Password policy simulation and analysis
Richard Shay, Abhilasha Bhargav-Spantzel, Elisa Bertino
November 2007 **Proceedings of the 2007 ACM workshop on Digital identity management DIM '07**
Publisher: ACM
Full text available: pdf(392.24 KB)   Additional Information: full citation, abstract, references, index terms

Passwords are an ubiquitous and critical component of many security systems. As the information and access guarded by passwords become more necessary, we become ever more dependent upon the security passwords provide. The creation and management of passwords is crucial, and for this we must develop and deploy password policies. This paper focuses on defining and modeling password policies for the entire password policy lifecycle. The paper first discusses a language for specifying password po ...

Keywords: management, modeling, password, policy, simulation

Results 1 - 20 of 200   Result page: **1** 2 3 4 5 6 7 8 9 10   next

Useful downloads: Adobe Acrobat   QuickTime   Windows Media Player   Real Player

Terms used: <u>**session**</u> <u>**key**</u> <u>**public**</u>
<u>**key**</u> <u>**password**</u> <u>**encode**</u> <u>**encrypt**</u> <u>**encipher**</u>

Found **1,133** of **216,412**

Sort results by [relevance   ▼]

Display results [expanded form ▼]

🖿 <u>Save results to a Binder</u>

[?] <u>Search Tips</u>

☐ Open results in a new window

Try an <u>Advanced Search</u>
Try this search in <u>The ACM Guide</u>

Results 1 - 20 of 200   Result page: **1** <u>2</u> <u>3</u> <u>4</u> <u>5</u> <u>6</u> <u>7</u> <u>8</u> <u>9</u> <u>10</u>   <u>next</u>

Best 200 shown

Relevance scale ☐ ▭ ▬ ◼ ◼

1 <u>Cryptography and data security</u>
Dorothy Elizabeth Robling Denning
January 1982 Book

Publisher: Addison-Wesley Longman Publishing Co., Inc.

Full text available: 🗎 <u>pdf(19.47 MB)</u>

Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>cited by</u>, <u>index terms</u>

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

2 <u>Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm</u>
Mihir Bellare, Tadayoshi Kohno, Chanathip Namprempre
May 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 2

Publisher: ACM Press

Full text available: 🗎 <u>pdf(404.99 KB)</u>

Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>, <u>review</u>

The *secure shell* (SSH) protocol is one of the most popular cryptographic protocols on the Internet. Unfortunately, the current SSH authenticated encryption mechanism is insecure. In this paper, we propose several fixes to the SSH protocol and, using techniques from modern cryptography, we prove that our modified versions of SSH meet strong new chosen-ciphertext privacy and integrity requirements. Furthermore, our proposed fixes will require relatively little modification to the SSH protoc ...

Keywords: Authenticated encryption, secure shell, security proofs, stateful decryption

3 <u>Encryption and Secure Computer Networks</u>

Gerald J. Popek, Charles S. Kline
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
Publisher: ACM Press
Full text available: pdf(2.50 MB)   Additional Information: full citation, references, citings, index terms

4   Symmetric and Asymmetric Encryption

Gustavus J. Simmons
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
Publisher: ACM Press
Full text available: pdf(2.23 MB)   Additional Information: full citation, references, citings, index terms

5   Public-key cryptography and password protocols

Shai Halevi, Hugo Krawczyk
August 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2
          Issue 3
Publisher: ACM Press

Full text available: pdf(275.84 KB)   Additional Information: full citation, abstract, references, citings, index
                                            terms, review

We study protocols for strong authentication and key exchange in asymmetric scenarios
where the authentication server possesses ~a pair of private and public keys while the
client has only a weak human-memorizable password as its authentication key. We
present and analyze several simple password authentication protocols in this scenario,
and show that the security of these protocols can be formally proven based on standard
cryptographic assumptions. Remarkably, our analysis shows optimal re ...

Keywords: dictionary attacks, hand-held certificates, key exchange, passwords, public
passwords, public-key protocols

6   A secure distributed capability based system (extended abstract)

Howard L. Johnson, John F. Koegel, Rhonda M. Koegel
October 1985 **Proceedings of the 1985 ACM annual conference on The range of
          computing : mid-80's perspective: mid-80's perspective ACM '85**
Publisher: ACM Press
Full text available: pdf(1.22 MB)   Additional Information: full citation, references, index terms

Keywords: capability architecture, computer security, distributed system security,
network encryption

7   Information security issues in an APL application

Bill Hillman
June 1984 **ACM SIGAPL APL Quote Quad , Proceedings of the international
          conference on APL APL '84**, Volume 14 Issue 4
Publisher: ACM Press
Full text available: pdf(549.98 KB)   Additional Information: full citation, abstract, references, index terms

This paper will describe various methods to secure an APL database application. Primary
foci will be in the areas of "physical" protection, and in cryptographic techniques. To that
end, distinctions will be made between "data," and "information." Because of those

differences, specific methods will be offered which are appropriate for each modality of security. A brief set of examples will be included for the use of IBM's1 RACF

8 Password Management and Digital Signatures: Delegation of cryptographic servers for capture-resilient devices
Philip MacKenzie, Michael K. Reiter
November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security CCS '01**
Publisher: ACM Press

Full text available: pdf(312.90 KB)   Additional Information: full citation, abstract, references, citings, index terms

A device that performs private key operations (signatures or decryptions), and whose private key operations are protected by a password, can be immunized against offline dictionary attacks in case of capture by forcing the device to confirm a password guess with a designated remote server in order to perform a private key operation. Recent proposals for achieving this allow untrusted servers and require no server initialization per device. In this paper we extend these proposals to enable dynami ...

9 Cryptographic protocols/ network security: Security proofs for an efficient password-based key exchange
Emmanuel Bresson, Olivier Chevassut, David Pointcheval
October 2003 **Proceedings of the 10th ACM conference on Computer and communications security CCS '03**
Publisher: ACM Press

Full text available: pdf(233.51 KB)   Additional Information: full citation, abstract, references, citings, index terms

Password-based key exchange schemes are designed to provide entities communicating over a public network, and sharing a (short) password only, with a session key (e.g, the key is used for data integrity and/or confidentiality). The focus of the present paper is on the analysis of very efficient schemes that have been proposed to the IEEE P1363 Standard working group on password-based authenticated key-exchange methods, but which actual security was an open problem. We analyze the AuthA key excha ...

Keywords: key exchange, password-based authentication

10 Modern trends in authentication
David L. Lipton, Harry K. T. Wong
September 1985 **ACM SIGSAC Review**, Volume 3 Issue 2-4
Publisher: ACM Press
Full text available: pdf(517.65 KB)   Additional Information: full citation, abstract, references

Authentication is the process of verifying a person's claim of identity. The designers of secure computer systems have incorporated many techniques of user-validation from law enforcement, from industrial security, and from the financial community. Several methods have also been developed explicitly for use in computer systems. This paper will present an overview of all methods of authentication currently used in computer security. Implementation considerations will also be discussed.

11 Public-key cryptography and password protocols
Shai Halevi, Hugo Krawczyk
November 1998 **Proceedings of the 5th ACM conference on Computer and communications security CCS '98**
Publisher: ACM Press
Full text available: pdf(1.28 MB)   Additional Information: full citation, references, citings, index terms

12 Separating key management from file system security

David Mazières, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchel
December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles SOSP '99**, Volume 33 Issue 5
Publisher: ACM Press

Full text available: pdf(1.77 MB)   Additional Information: full citation, abstract, references, citings, index terms

> No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security at a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use.We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal ...

13 Cryptography: Password authenticated key exchange using hidden smooth subgroups

Craig Gentry, Philip Mackenzie, Zulfikar Ramzan
November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**
Publisher: ACM Press

Full text available: pdf(300.13 KB)   Additional Information: full citation, abstract, references, citings, index terms

> Existing techniques for designing efficient password authenticated key exchange (PAKE) protocols all can be viewed as variations of a small number of fundamental paradigms, and all are based on either the Diffie-Hellman or RSA assumptions. In this paper we propose a new technique for the design of PAKE protocols that does not fall into any of those paradigms, and which is based on a different assumption. In our technique, the server uses the password to construct a multiplicative group with a (h ...

Keywords: authentication, cryptography, key exchange, password

14 Secure sessions for Web services

Karthikeyan Bhargavan, Ricardo Corin, Cédric Fournet, Andrew D. Gordon
May 2007 **ACM Transactions on Information and System Security (TISSEC)**, Volume 10 Issue 2
Publisher: ACM Press

Full text available: pdf(579.98 KB)   Additional Information: full citation, abstract, references, index terms

> We address the problem of securing sequences of SOAP messages exchanged between web services and their clients. The WS-Security standard defines basic mechanisms to secure SOAP traffic, one message at a time. For typical web services, however, using WS-Security independently for each message is rather inefficient; moreover, it is often important to secure the integrity of a whole session, as well as each message. To these ends, recent specifications provide further SOAP-level mechanisms. WS-S ...

Keywords: Web services, XML security

15 Secure password-based cipher suite for TLS

May 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 2

Publisher: ACM Press

Full text available: 🔁 pdf(507.57 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>, <u>review</u>

SSL is the de facto standard today for securing end-to-end transport on the Internet. While the protocol itself seems rather secure, there are a number of risks that lurk in its use, for example, in web banking. However, the adoption of password-based key-exchange protocols can overcome some of these problems. We propose the integration of such a protocol (DH-EKE) in the TLS protocol, the standardization of SSL by IETF. The resulting protocol provides secure mutual authentication and key establi ...

Keywords: Authenticated key exchange, dictionary attack, key agreement, password, perfect forward secrecy, secure channel, transport layer security, weak secret

16 <u>Computer security (SEC): Protected transmission of biometric user authentication</u> ■
<u>data for oncard-matching</u>
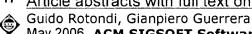Ulrich Waldmann, Dirk Scheuermann, Claudia Eckert
March 2004 **Proceedings of the 2004 ACM symposium on Applied computing SAC '04**
Publisher: ACM Press
Full text available: 🔁 pdf(574.45 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>

Since fingerprint data are no secrets but of public nature, the verification data transmitted to a smartcard for oncard-matching need protection by appropriate means in order to assure data origin in the biometric sensor and to prevent bypassing the sensor. For this purpose, the verification data to be transferred to the user smartcard is protected with a cryptographic checksum that is calculated within a separate security module controlled by a tamper resistant card terminal with integrated bio ...

Keywords: authentication, biometrics, cryptographic protocols, data integrity, electronic signature, oncard-matching, smartcards, system security, tamper proof environment

17 <u>Article abstracts with full text online: A consistent history authentication protocol</u> ■
Guido Rotondi, Gianpiero Guerrera
May 2006 **ACM SIGSOFT Software Engineering Notes**, Volume 31 Issue 3
Publisher: ACM Press
Full text available: 🔁 pdf(287.59 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

Traditional strong authentication systems rely on a certification chain to delegate the authority of trusting an intermediate end. However, in some practical life scenarios a relayed authentication is not accepted and thus it would be advisable a straight proof of trustiness with a direct interaction with the involved party. Our protocol introduces a registry of certified operations from which it descends the authentication and the consequent proof of identity. Despite the fact that such system ...

Keywords: SSL, authentication, dentification, non repudiation, trust

18 <u>Role-based access control on the web</u> ■
Joon S. Park, Ravi Sandhu, Gail-Joon Ahn
February 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 1
Publisher: ACM Press

Full text available: 🔁 pdf(331.03 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>, <u>review</u>

Current approaches to access control on the Web servers do not scale to enterprise-wide

systems because they are mostly based on individual user identities. Hence we were motivated by the need to manage and enforce the strong and efficient RBAC access control technology in large-scale Web environments. To satisfy this requirement, we identify two different architectures for RBAC on the Web, called user-pull and server-pull. To demonstrate feasibility, we im ...

Keywords: WWW security, cookies, digital certificates, role-based access control

19 Secure sessions for web services

Karthikeyan Bhargavan, Ricardo Corin, Cédric Fournet, Andrew D. Gordon
October 2004 **Proceedings of the 2004 workshop on Secure web service SWS '04**
Publisher: ACM Press
Full text available: pdf(351.35 KB)   Additional Information: full citation, abstract, references, citings

WS-Security provides basic means to secure SOAP traffic, one envelope at a time. For typical web services, however, using WS-Security independently for each message is rather inefficient; besides, it is often important to secure the integrity of a whole session, as well as each message. To these ends, recent specifications provide further SOAP-level mechanisms. WS-SecureConversation introduces *security contexts*, which can be used to secure sessions between two parties. WS-Trust specifies ...

20 Identification control: Public key distribution through "cryptoIDs"

Trevor Perrin
August 2003 **Proceedings of the 2003 workshop on New security paradigms NSPW '03**
Publisher: ACM Press
Full text available: pdf(1.51 MB)   Additional Information: full citation, abstract, references, citings, index terms

In this paper, we argue that person-to-person key distribution is best accomplished with a key-centric approach, instead of PKI: users should distribute public key fingerprints in the same way they distribute phone numbers, postal addresses, and the like. To make this work, fingerprints need to be *small*, so users can handle them easily; *multipurpose*, so only a single fingerprint is needed for each user; and *long-lived*, so fingerprints don't have to be frequently redistribute ...

Keywords: cryptoIDs, fingerprints, key distribution, key management, public key infrastructure

Results 1 - 20 of 200   Result page: **1** 2 3 4 5 6 7 8 9 10 next

PⓈRTAL

USPTO

Search: ⊙ The ACM Digital Library   ○ The Guide

`+asymmetric +key +pair password`   **SEARCH**

THE ACM DIGITAL LIBRARY

📌 Feedback Report a problem Satisfaction survey

Terms used: **asymmetric key pair password**   Found **1,611** of **216,412**

Sort results by   `relevance ▼`   🔖 Save results to a Binder   Try an Advanced Search
Display results   `expanded form ▼`   ❓ Search Tips   Try this search in The ACM Guide
                                         ☐ Open results in a new
                                         window

Results 1 - 20 of 200   Result page: **1** 2 3 4 5 6 7 8 9 10   next
Best 200 shown   Relevance scale ☐▭▬■■

1 **Public-key cryptography and password protocols**   ■

Shai Halevi, Hugo Krawczyk
August 1999 **ACM Transactions on Information and System Security (TISSEC),** Volume 2
         Issue 3
Publisher: ACM Press

Full text available: 🗎 pdf(275.84 KB)   Additional Information: full citation, abstract, references, citings, index
                                                              terms, review

> We study protocols for strong authentication and key exchange in asymmetric scenarios
> where the authentication server possesses ~a pair of private and public keys while the
> client has only a weak human-memorizable password as its authentication key. We
> present and analyze several simple password authentication protocols in this scenario,
> and show that the security of these protocols can be formally proven based on standard
> cryptographic assumptions. Remarkably, our analysis shows optimal re ...

Keywords: dictionary attacks, hand-held certificates, key exchange, passwords, public
passwords, public-key protocols

2 **Public-key cryptography and password protocols**   ■
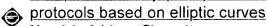
Shai Halevi, Hugo Krawczyk
November 1998 **Proceedings of the 5th ACM conference on Computer and
                communications security CCS '98**
Publisher: ACM Press
Full text available: 🗎 pdf(1.28 MB)   Additional Information: full citation, references, citings, index terms

3 **Computer security (SEC): Efficient Diffie-Hellmann two-party key agreement**   ■

protocols based on elliptic curves
Maurizio Adriano Strangio
March 2005 **Proceedings of the 2005 ACM symposium on Applied computing SAC '05**
Publisher: ACM Press
Full text available: 🗎 pdf(234.27 KB)   Additional Information: full citation, abstract, references, index terms

> Key agreement protocols are of fundamental importance for ensuring the confidentiality of
> communications between two (or more) parties over an insecure network. In this paper
> we review existing two-party protocols whose security rests upon the intractability of
> Diffie-Hellmann and Discrete Logarithm problems over elliptic curve groups. In addition,

we propose a new two-party mutual authenticated key agreement protocol and collectively evaluate the security and performance of all the schemes cons ...

Keywords: cryptography, elliptic curves, key agreement, protocols

4 Accountability protocols: Formalized and verified

Giampaolo Bella, Lawrence C. Paulson

May 2006 **ACM Transactions on Information and System Security (TISSEC)**, Volume 9 Issue 2

Publisher: ACM Press

Full text available: pdf(433.82 KB)   Additional Information: full citation, abstract, references, index terms

Classical security protocols aim to achieve authentication and confidentiality under the assumption that the peers behave honestly. Some recent protocols are required to achieve their goals even if the peer misbehaves. *Accountability* is a protocol design strategy that may help. It delivers to peers sufficient evidence of each other's participation in the protocol. Accountability underlies the nonrepudiation protocol of Zhou and Gollmann and the certified email protocol of Abadi et al. Thi ...

Keywords: Isabelle, Nonrepudiation, certified email, inductive method, proof tools

5 Research contibutions: A review of information security issues and respective research contributions

Mikko T. Siponen, Harri Oinas-Kukkonen

February 2007 **ACM SIGMIS Database**, Volume 38 Issue 1

Publisher: ACM Press

Full text available: pdf(353.82 KB)   Additional Information: full citation, abstract, references, index terms

This paper identifies four security issues (access to Information Systems, secure communication, security management, development of secure Information Systems), and examines the extent to which these security issues have been addressed by existing research efforts. Research contributions in relation to these four security issues are analyzed from three viewpoints: a meta-model for information systems, the research approaches used, and the reference disciplines used. Our survey reveals that most ...

Keywords: computer science

6 Public-key cryptography and password protocols: the multi-user case

Maurizio Kliban Boyarsky

November 1999 **Proceedings of the 6th ACM conference on Computer and communications security CCS '99**

Publisher: ACM Press

Full text available: pdf(1.00 MB)   Additional Information: full citation, abstract, references, citings, index terms

The problem of password authentication over an insecure network when the user holds only a human-memorizable password has received much attention in the literature. The first rigorous treatment was provided by Halevi and Krawczyk, who studied off-line password guessing attacks in the scenario in which the authentication server possesses a pair of private and public keys. In this work we: Show the inadequacy of both the HK formalization and protocol in the ...

7 Applications and compliance: TCG inside?: a note on TPM specification compliance

Ahmad-Reza Sadeghi, Marcel Selhorst, Christian Stüble, Christian Wachsmann, Marcel

Winandy, Horst Görtz
November 2006 **Proceedings of the first ACM workshop on Scalable trusted computing**
          STC '06
Publisher: ACM Press
Full text available: pdf(587.22 KB)   Additional Information: full citation, abstract, references, index terms

>The Trusted Computing Group (TCG) has addressed a new generation of computing
>platforms employing both supplemental hardware and software with the primary goal to
>improve the security and the trustworthiness of future IT systems. The core component of
>the TCG proposal is the Trusted Platform Module (TPM) providing certain cryptographic
>functions. Many vendors currently equip their platforms with a TPM claiming to be TCG
>compliant. However, there is no feasible way for application developers and ...

>**Keywords:** TPM, compliance, test, trusted computing

8 A framework for password-based authenticated key exchange[1]   ◼
Rosario Gennaro, Yehuda Lindell
May 2006 **ACM Transactions on Information and System Security (TISSEC)**, Volume 9
          Issue 2
Publisher: ACM Press
Full text available: pdf(574.64 KB)   Additional Information: full citation, abstract, references, index terms

>In this paper, we present a general framework for password-based authenticated key
>exchange protocols, in the common reference string model. Our protocol is actually an
>abstraction of the key exchange protocol of Katz et al. and is based on the recently
>introduced notion of smooth projective hashing by Cramer and Shoup. We gain a number
>of benefits from this abstraction. First, we obtain a modular protocol that can be described
>using just three high-level cryptographic tools. This allows a simpl ...

>**Keywords:** Passwords, authentication, dictionary attack, projective hash functions

9 Introduction of the asymmetric cryptography in GSM, GPRS, UMTS, and its public   ◼
key infrastructure integration
Constantinos F. Grecas, Sotirios I. Maniatis, Iakovos S. Venieris
April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2
Publisher: Kluwer Academic Publishers
Full text available: pdf(107.24 KB)   Additional Information: full citation, abstract, references, index terms

>The logic ruling the user and network authentication as well as the data ciphering in the
>GSM architecture is characterized, regarding the transferring of the parameters employed
>in these processes, by transactions between three nodes of the system, that is the MS,
>actually the SIM, the visited MSC/VLR, and the AuC, which is attached to the HLR in most
>cases. The GPRS and the UMTS architecture carry the heritage of the GSM's philosophy
>regarding the user/network authentication and the data ciphe ...

>**Keywords:** PKIs, PLMNs, asymmetric cryptography

10 CMOS & logic applications optimization and techniques: Design of an UHF RFID   ◼
transponder for secure authentication
Paolo Bernardi, Filippo Gandino, Bartolomeo Montrucchio, Maurizio Rebaudengo, Erwing
Ricardo Sanchez
March 2007 **Proceedings of the 17th great lakes symposium on Great lakes
          symposium on VLSI GLSVLSI '07**
Publisher: ACM Press

Full text available: 📄 pdf(347.57 KB)   Additional Information: full citation, abstract, references, index terms

RFID technology increases rapidly its applicability in new areas of interest without guaranteeing security and privacy issues. This paper presents a new architecture of an RFID transponder with cryptographic capabilities. Other than being compatible with the EPC Class-1 Gen-2 communication protocol, our tag implements an asymmetric ciphering module that proved useful in authentication and anti-counterfeit schemes, particularly critical in many application fields. Experimental results concerning ...

Keywords: RFID, authentication, privacy

11 Protecting applications with transient authentication

Mark D. Corner, Brian D. Noble
May 2003 **Proceedings of the 1st international conference on Mobile systems, applications and services MobiSys '03**
Publisher: ACM Press
Full text available: 📄 pdf(294.40 KB)   Additional Information: full citation, abstract, references, cited by

How does a machine know who is using it? Current systems authenticate their users infrequently, and assume the user's identity does not change. Such *persistent authentication* is inappropriate for mobile and ubiquitous systems, where associations between people and devices are fluid and unpredictable. We solve this problem with *Transient Authentication*, in which a small hardware token continuously authenticates the user's presence over a short-range, wireless link. We present the fo ...

12 Asymmetric fingerprinting for larger collusions

Birgit Pfitzmann, Michael Waidner
April 1997 **Proceedings of the 4th ACM conference on Computer and communications security CCS '97**
Publisher: ACM Press
Full text available: 📄 pdf(1.37 MB)   Additional Information: full citation, references, citings, index terms

13 Symmetric and Asymmetric Encryption

Gustavus J. Simmons
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
Publisher: ACM Press
Full text available: 📄 pdf(2.23 MB)   Additional Information: full citation, references, citings, index terms

14 Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise

Steven M. Bellovin, Michael Merritt
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security CCS '93**
Publisher: ACM Press
Full text available: 📄 pdf(620.09 KB)   Additional Information: full citation, abstract, references, citings, index terms

The encrypted key exchange (EKE) protocol is augmented so that hosts do not store cleartext passwords. Consequently, adversaries who obtain the one-way encrypted password file may (i) successfully mimic (spoof) the host to the user, and (ii) mount dictionary attacks against the encrypted passwords, but cannot mimic the user to the host. Moreover, the important security properties of EKE are preserved—an active

network attacker obtains insufficient information to mount dictionary attac ...

15 Smart Cards and Biometrics: The cool way to make secure transactions
David Corcoran, David Sims, Bob Hillhouse
March 1999 **Linux Journal**
Publisher: Specialized Systems Consultants, Inc.
Full text available: html(22.95 KB)   Additional Information: full citation, index terms

16 Cryptography and data security
Dorothy Elizabeth Robling Denning
January 1982 Book
Publisher: Addison-Wesley Longman Publishing Co., Inc.
Full text available: pdf(19.47 MB)   Additional Information: full citation, abstract, references, cited by, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

17 Cryptographic protocols/ network security: Security proofs for an efficient password-based key exchange
Emmanuel Bresson, Olivier Chevassut, David Pointcheval
October 2003 **Proceedings of the 10th ACM conference on Computer and communications security CCS '03**
Publisher: ACM Press
Full text available: pdf(233.51 KB)   Additional Information: full citation, abstract, references, citings, index terms

Password-based key exchange schemes are designed to provide entities communicating over a public network, and sharing a (short) password only, with a session key (e.g, the key is used for data integrity and/or confidentiality). The focus of the present paper is on the analysis of very efficient schemes that have been proposed to the IEEE P1363 Standard working group on password-based authenticated key-exchange methods, but which actual security was an open problem. We analyze the AuthA key excha ...

Keywords: key exchange, password-based authentication

18 Identification and authentication when users have multiple accounts
W. R. Shockley
August 1993 **Proceedings on the 1992-1993 workshop on New security paradigms NSPW '92-93**
Publisher: ACM Press
Full text available: pdf(788.71 KB)   Additional Information: full citation, references

19 Secret key distribution protocol using public key cryptography

Amit Parnerkar, Dennis Guster, Jayantha Herath
October 2003 **Journal of Computing Sciences in Colleges**, Volume 19 Issue 1
Publisher: Consortium for Computing Sciences in Colleges
Full text available: [icon] pdf(74.93 KB)   Additional Information: full citation, abstract, references, index terms

This paper presents the description and analysis of a protocol, which uses hybrid crypto algorithms for key distribution. A triple DES with a 168-bit key is used to generate the secret key. This secret key is transferred with the help of public key cryptography. The authentication process is accomplished by using the message digest algorithm MD5. This protocol uses mutual authentication in which, both participants have to authenticate themselves via a third trusted certificate authority (CA). Th ...

20 Password Management and Digital Signatures: Delegation of cryptographic servers   [icon]
for capture-resilient devices
Philip MacKenzie, Michael K. Reiter
November 2001 **Proceedings of the 8th ACM conference on Computer and
Communications Security CCS '01**
Publisher: ACM Press

Full text available: [icon] pdf(312.90 KB)   Additional Information: full citation, abstract, references, citings, index terms

A device that performs private key operations (signatures or decryptions), and whose private key operations are protected by a password, can be immunized against offline dictionary attacks in case of capture by forcing the device to confirm a password guess with a designated remote server in order to perform a private key operation. Recent proposals for achieving this allow untrusted servers and require no server initialization per device. In this paper we extend these proposals to enable dynami ...

Results 1 - 20 of 200   Result page: **1** 2 3 4 5 6 7 8 9 10   next

Useful downloads: [icon] Adobe Acrobat   [icon] QuickTime   [icon] Windows Media Player   [icon] Real Player

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	2	"5421599".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/08 12:13
S2	2	"5421599".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/08 12:14
S3	2	"5421559".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/08 12:14
S4	2	"5241559".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/08 12:14
S5	2	"5241599".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/09 12:03
S6	368	port with (change$2 alter$2 modif$3) with number$2 and HTTP	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/09 12:04
S7	170	port near3 (change$2 alter$2 modif$3) with number$2 and HTTP	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/09 12:04
S8	22	port near3 (change$2 alter$2 modif$3) with number$2 and HTTP and HTTP and SSL	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/09 12:08

S9	1078	port near3 (change$2 alter$2 modif$3 setting) with number$2	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/09 12:09
S10	17	port near3 (change$2 alter$2 modif$3 setting) with number$2 same (port adj "80")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/09 12:09
S11	12	port near3 (change$2 alter$2 modif$3 setting) with number$2 same (port adj "80") same (HTTPS SSL HTTP)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/09 12:10
S12	1	simms.in. and (ESTABLISHING adj SECURE adj COMMUNICATION).ti.	US-PGPUB	OR	OFF	2006/09/27 14:09
S13	401	380/285.ccls. 380/283.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 18:41
S14	287	380/285.ccls. 380/283.ccls. and (random adj number)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/27 14:11
S15	245	380/285.ccls. 380/283.ccls. and (random adj number) and (public adj key)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/27 14:12
S16	142	(380/285.ccls. 380/283.ccls.) and (random adj number) and (public adj key)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/27 14:14
S17	6	(380/285.ccls. 380/283.ccls.) and (random adj number) and (public adj key) and (calling adj party)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/27 14:43

EAST Search History

S18	107	(key with establish$4) same (random adj number) same (public adj key)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/27 15:16
S19	79	(key with establish$4) same (random adj number) same (public adj key) same (encrypt$4 encode$4)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/27 15:24
S20	2	(identity adj verification$) with (online adj bank$4)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/27 15:27
S21	0	(security$4 near2 question$2) same (password adj retrieval)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/27 15:28
S22	105	(security$4 near2 question$2) same (password)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/27 17:13
S23	4	"6189098".pn. "6886095".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/27 21:39
S24	1030	session adj key with (establish$5 agreement$4)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/27 21:40
S25	168	session adj key with (establish$5 agreement$4) and (random adj number$4) with (first second)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/27 21:40

EAST Search History

S26	15	session adj key with (establish$5 agreement$4) and (random adj number$4) with (first second) near30 (public adj key)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/28 11:10
S27	85	mutual$2 adj authenticat$4 same (random$2 adj number$4) same (public adj key)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/28 11:13
S28	5	mutual$2 adj authenticat$4 same (random$2 adj number$4) same (public adj key) same (symmetric adj key)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/28 11:14
S29	5	mutual$2 adj authenticat$4 same (random$2 adj number$4) same (public adj key) same (symmetric adj key) and (session adj key)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/28 11:15
S30	116	session adj key same (random adj number) with (first) with (second)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/28 11:15
S31	73	S30 and (public adj key)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/28 11:16
S32	48	S30 and (public adj key) and (password (symmetric adj key))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/28 14:42
S33	2	"6539749".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/28 14:43

EAST Search History

S34	2	"6539479".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/28 14:43
S35	217	380/285.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 18:41
S36	280	380/283.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 18:41
S37	731	713/150.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 18:42
S38	2118	713/168.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 18:42
S39	881	713/171.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 19:38
S40	509	380/255.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 19:39
S41	4169	S35 S36 S37 S38 S39 S40	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 19:49

EAST Search History

S42	1426	S41 and (random$ adj number$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 19:50
S43	57	S42 and ((encod$3 encrypt$4) adj password$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 19:54
S44	43	S43 and ((public private) near2 key$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 19:56
S45	12	S43 and (session adj key$2) with (establish$5 creat$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 19:58
S46	57	S43 and ((encod$3 encipher$2 encrypt$4) near2 password$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 20:00
S47	10	S43 and (shared$2 with (secret$4 adj key))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 20:05
S48	620	S41 and (password) and (public adj key) and (private adj key)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 20:06
S49	348	S41 and (password) and (public adj key) and (private adj key) and ((session shared) near3 (key))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 20:08

EAST Search History

S50	224	S41 and (password) and (public adj key) and (private adj key) and ((session shared) near3 (key)) and hash$2	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/02 20:09
S51	4	PLETHORA.as.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/03 15:41
S52	2	timothy near3 simms.in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/03 15:42
S53	2	"5835592".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/03 16:18
S54	217	380/285.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/03 16:18
S55	280	380/283.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/03 16:18
S56	733	713/150.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/03 16:18
S57	2122	713/168.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/03 16:18

EAST Search History

S58	884	713/171.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/03 16:18
S59	509	380/255.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/03 16:18
S60	4178	S54 S55 S56 S57 S58 S59	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/03 16:18
S61	4178	S60	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/03 16:18
S62	934	S60 and (public adj key).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/03 16:18
S63	15	S60 and (public adj key).clm. and ((encod$3 encrypt$4 encipher$2) near2 (password$2)).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/03 16:19